J8 Security Document Artwork That Resists Reverse Engineering

Joel A. Zlotnick, MSFS, US Department of State, 600 19th Street, NW, Ste 12.601, Washington, DC 20522; Jordan C. Brough, MFS, HSI Forensic Laboratory, 8000 Westpark Drive, Ste 325, McLean, VA 22102; and Troy J. Eberhardt, BS, 14931 Greymont Drive, Centreville, VA 20120-1519*

After attending this presentation, attendees will understand how design strategies for security document artwork can play a key role in the prevention of artwork reverse engineering by sophisticated traditional counterfeiters.

This presentation will impact the forensic science community by demonstrating novel strategies for the design of artwork in security documents and how forensic examination of document artwork could be impacted in the future if there is some adoption of this novel design paradigm.

Counterfeiting can be accomplished via one of two basic workflows: digital and traditional. The easier scan-and-print workflow of digital counterfeiting has made counterfeiting easier and more accessible to criminals with limited graphic art skills because it does not require counterfeiters to redraw document artwork, manufacture printing plates, or operate a printing press; however, digital counterfeiting processes are only capable of simulating document artwork using inkjet or toner devices. This places limitations on the quality of the counterfeits that can be produced by digital counterfeiting because the printing process characteristics of the letterpress, intaglio, and lithographic printing processes used to produce genuine security documents cannot be fully replicated with computer printers, office copiers, or multifunction devices.

In contrast, traditional counterfeiters follow a more sophisticated and technically demanding workflow that has the potential to produce counterfeits of higher quality. Traditional counterfeiters try to mimic not just the basic appearance of the document but also the combination of printing processes used in its manufacturing. Before any redrawing or replication of document artwork can proceed, traditional counterfeiters must reverse engineer the artwork to determine how many different printing plates were used, the specific artwork featured on each plate, and other production parameters. Once the counterfeiter understands how a genuine document was printed, it becomes possible to replicate the document artwork, even if executing the replication is made more difficult because of printed security features such as line art, spot colors, microprinting, guilloche patterns, split fountain printing, latent images, transparent register, and similar features.

The security artwork strategies described above all increase the difficulty of either generating the artwork or physically printing the artwork on press. Importantly, not one of these strategies is deliberately targeted at the prepress process of separating the individual printing plate images, which means that a number of theoretical strategies that do target this particular process remain largely unexplored in the contemporary practice of security document design. If a counterfeiter is unable to determine the number of printing plates used or the specific artwork present on each plate, then there is no pathway toward accurate replication of the individual plate artwork. At best, the counterfeiter abandons the attack or, at worst, must compromise the quality of the counterfeit. The question is how to use design to force traditional counterfeiters to face these complications.

To understand how a genuine document was printed, traditional counterfeiters rely on a series of four visual cues that are present in the artwork of most historical and contemporary security documents. These cues include the printing of different colors of ink from each separate plate, the use of continuous line patterns that can be traced, delivery of complete artwork visual elements from a single printing plate, and the use of different artwork styles on different printing plates. Therefore, purposefully designing artwork that does not contain these four cues can produce security designs that can be originated and printed by genuine document issuers, but which are very challenging to reverse engineer if starting only from the printed hardcopy document, as a counterfeiter must. Such designs are essentially the opposite of the four cues described above; they contain the same color of ink on each printing plate, continuous line patterns are eliminated or minimized, most artwork elements require multiple plate images to produce, and the same basic artwork style is used across all printing plates.

This presentation will describe these design techniques, provide examples of security artwork concepts that comply with these principles, and explain ramifications for forensic examination of security document artwork.

Counterfeit, Artwork, Design

*Presenting Author